SPYWOLF

Security Audit Report

Completed on
December 14, 2022

OVERVIEW

This audit has been prepared for **DOGEPAD** to review the main aspects of the project to help investors make make an informative decision during their research process.

You will find a a summarized review of the following key points:

- ✔ Contract's source code
- ✔ Owners' wallets
- ✔ Tokenomics
- ✔ Team transparency and goals
- ✔ Website's age, code, security and UX
- ✔ Whitepaper and roadmap
- ✔ Social media & online presence

The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal

– SPYWOLF Team –

TABLE OF CONTENTS

DOGEPAD

PROJECT DESCRIPTION

According to their whitepaper:

$DPF is Meme Inspired and Utility Driven. A diverse multichain DEFI ecosystem which offers multiple short and long term utility alongside a popular meme concept. $DPX represents a collective of people with a passion to succeed and a united set of goals.

Release Date: Launched at December 12, 2022
Category: DEFI

01

CONTRACT INFO

Token Name
DogepadStaking

Symbol
N/A

Contract Address
0xEdcd4AD478B75e44Ee10b90f8232526B6F128391

Network
Binance Smart Chain

Language
Solidity

Deployment Date
Dec 13, 2022

Verified?
Yes

Total Supply
Staking contract

Status
Deployed

TAXES

Buy Tax
2%

Sell Tax
2%

*Taxes can be changed in future

Our Contract Review Process

The contract review process pays special attention to the following:

- ✓ Testing the smart contracts against both common and uncommon vulnerabilities
- ✓ Assessing the codebase to ensure compliance with current best practices and industry standards.
- ✓ Ensuring contract logic meets the specifications and intentions of the client.
- ✓ Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- ✓ Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

02

CURRENT STATS

(As of December 14, 2022)

Liquidity

Not added yet

Burn

No burnt tokens

Status:
Not Launched!

MaxTxAmount
No limit

Additional Information

LP Address(es)

This is a staking contract - no liquidity required

Stake token:
0x182fd4f68695f1951018b5f8c1b2f778919ff0ce ($DPF)

TOKEN TRANSFERS STATS

Transfer Count	N/A
Uniq Senders	N/A
Uniq Receivers	N/A
Total Amount	N/A
Median Transfer Amount	N/A
Average Transfer Amount	N/A
First transfer date	N/A
Last transfer date	N/A
Days token transferred	N/A

SMART CONTRACT STATS

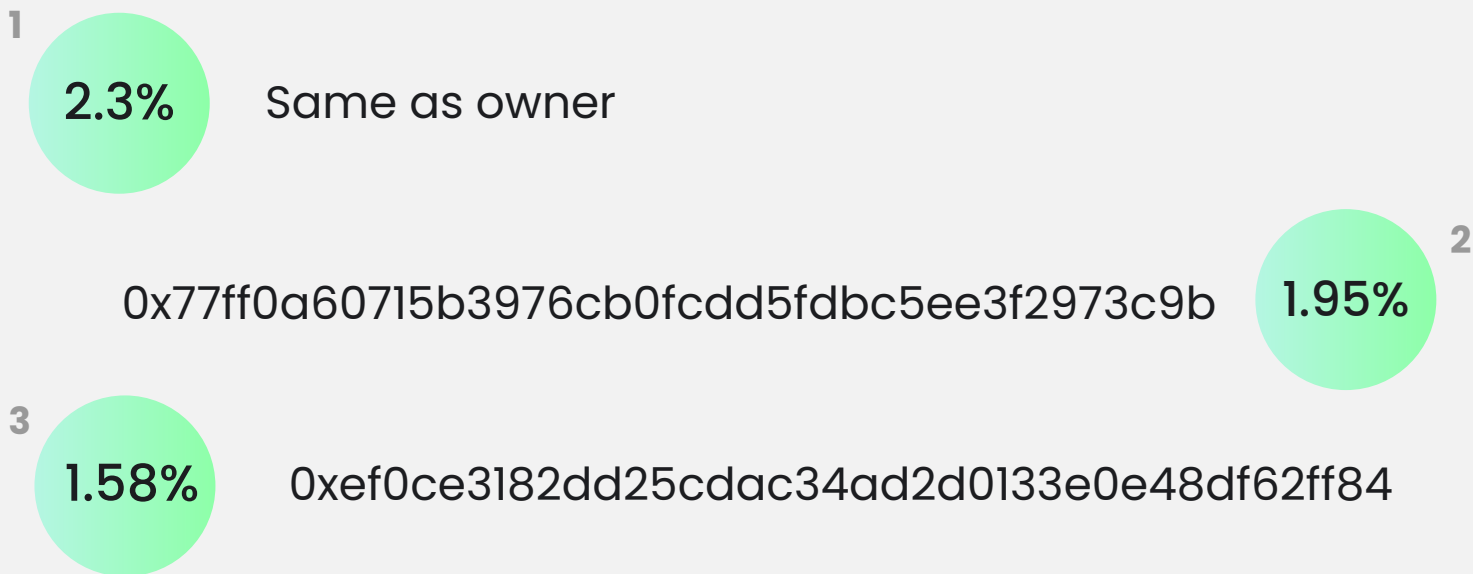|	
Calls Count	1
External calls	1
Internal calls	0
Transactions count	1
Uniq Callers	1
Days contract called	1
Last transaction time	2022-12-13 16:50:10 UTC
Created	2022-12-13 16:50:10 UTC
Create TX	0x83b5a5b645b85633f6552c893ce80efb009c7facd1d549d0784ee1b8548d1680
Creator	0x4b371a173ce974059f43d8219cfc1972187822a8

04

FEATURED WALLETS

Owner address	0x33a1fa5cbc6a5e6c0fffa0849325d52d9e9a9224
LP address	**This is staking contract, no liquidity required.**

TOP 3 UNLOCKED WALLETS

Information below is for holders of the current staking token (0x182FD4f68695F1951018B5f8C1B2F778919FF0CE)

1

2.3% Same as owner

2

0x77ff0a60715b3976cb0fcdd5fdbc5ee3f2973c9b **1.95%**

3

1.58% 0xef0ce3182dd25cdac34ad2d0133e0e48df62ff84

05

VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed

THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

FOUND THREATS

⚠️ High Risk

Owner can set percent divider without limitations.
If set to 0, the functions that uses it to calculate percentages will fail (impossible division by zero).
This variable is also responsible for calculations of the staking rewards and deposit/withdraw fees.

```
function SetDivider(uint256 percent) external onlyowner {
    percentDivider = percent;
}

uint256[2] public Bonus = [96, 384];

function stake(uint256 amount, uint256 planIndex) public {
...............
stakersRecord[msg.sender][index].reward = amount
.mul(Bonus[planIndex])
.div(percentDivider);
...............
}
```

- Recommendation:
  - Considered as good practice is divider to be constant.

08-A

FOUND THREATS

⚠️ High Risk

Owner can set deposit/withdraw fees without limitation.
It can be set to 100% and withdraw will become impossible.

```
function SetFee(uint256 percent1, uint256 percent2) external onlyowner {
    depositFee = percent1;
    withdrawFee = percent2;
}
```

- Recommendation:
  - Considered as good tax deduction practice is deposit and withdraw fees combined not to exceed 25%.

08-B

FOUND THREATS

⚠️ High Risk

Owner can set staking reward duration criteria without limitation.
If set to 0, functions relying on it will fail (division by zero is impossible).

```solidity
function SetTime(uint256 time) external onlyowner {
    timePeriod = time;
}

function unstake(uint256 index) public {
........
uint256 claimableReward;
if (block.timestamp < stakersRecord[msg.sender][index].withdrawtime) {
    uint256 duration = (block.timestamp -
    stakersRecord[msg.sender][index].staketime) / timePeriod;
    claimableReward =
    duration *
    stakersRecord[msg.sender][index].perDayReward;
}
........
}

function stake(uint256 amount, uint256 planIndex) public {
........
stakersRecord[msg.sender][index].perDayReward = stakersRecord[
    msg.sender
][index].reward.div(Duration[planIndex].div(timePeriod));
........
}
```

- Recommendation:
  - Consider to set limiter with reasonable number for the lower and upper values of timePeriod variable.

08-C

FOUND THREATS

⚠️ Medium Risk

Owner can change stake duration plans period without limitation.
Owner can change staking bonus without limitation.
If set to 0, no rewards will be paid to users.

```solidity
function SetStakeDuration(uint256 first, uint256 second)
    external
    onlyowner
{
    Duration[0] = first;
    Duration[1] = second;
}

function SetStakeBonus(uint256 first, uint256 second) external onlyowner {
    Bonus[0] = first;
    Bonus[1] = second;
}
```

- Recommendation:
  - Consider to set limiter with reasonable number for the lower and upper values, for both staking duration plans and staking bonus rewards.

RECOMMENDATIONS FOR

GOOD PRACTICES

1 Consider fundamental tradeoffs

2 Be attentive to blockchain properties

3 Ensure careful rollouts

4 Keep contracts simple

5 Stay up to date and track development

Dogepad Staking
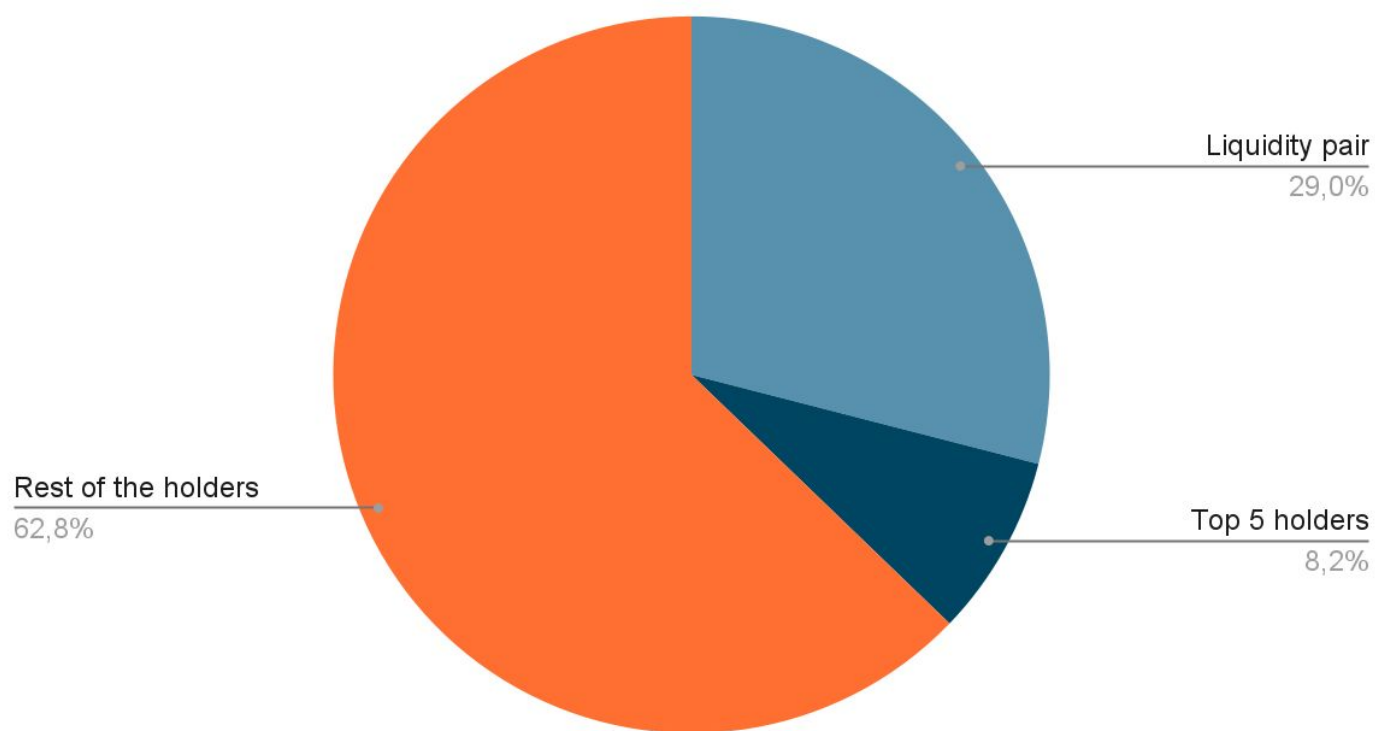
GOOD PRACTICES FOUND

✔ The smart contract utilizes "SafeMath" to prevent overflows

09

The following tokenomics are for the current staking token ($DPF):

- 29% - Liquidity pair
- 8.2% - Top 5 holders
- 62.8% - Rest of the holders

Tokens distribution

Liquidity pair
29,0%

Top 5 holders
8,2%

Rest of the holders
62,8%

THE TEAM

The team has privately doxxed to PINKSALE

https://pinksale.notion.site/DogePad-Finance-KYC-Verification-fb84553fa96e47fa93ac0591399a69e8

DogePad Finance - KYC Verification

This KYC page verifies that One Member of the project has successfully completed the verification process at PinKSale. Project info:

- Project Name: DogePad Finance
- Project Website: http://dogepad.pro/
- KYC Issued: November 30, 2022

Website URL
http://dogepad.pro/

Domain Registry
https://www.namecheap.com/

Domain Expiration
Expires on 2023-11-21

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

Design
Nice design with appropriate color scheme and graphics.

Content
The information helps new investors understand what the product does right away. No grammar mistakes found.
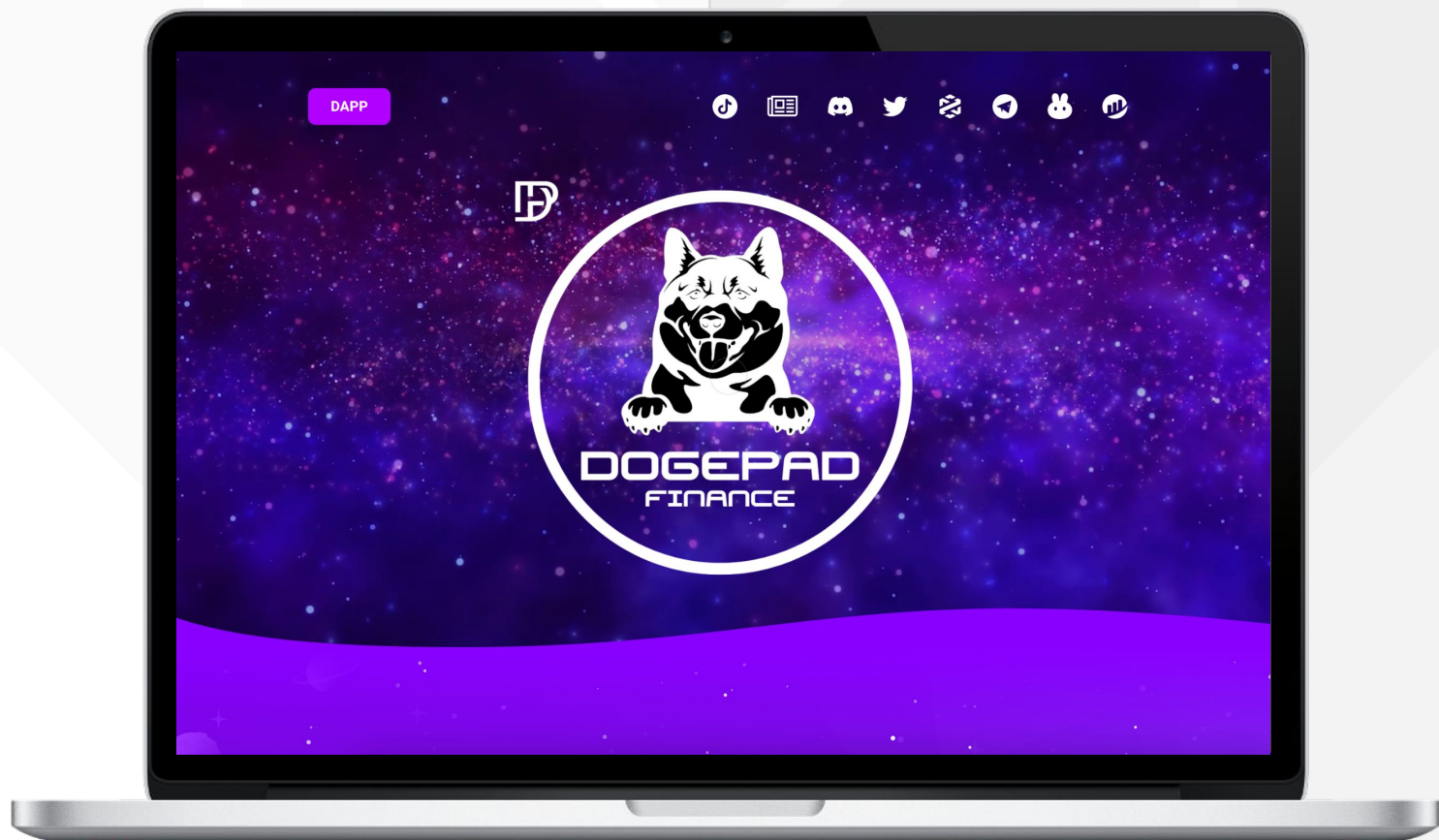
Whitepaper
Well written, explanatory.

Roadmap
Yes, goals set at 4 phases

Mobile-friendly?
Yes

dogepad.pro

SOCIAL MEDIA
& ONLINE PRESENCE

Twitter

@Dogepadfinance

- 2 231 followers
- Active
- Posts frequently

Discord

https://discord.com/invite/TaNcE6UT

- 437 members
- Active members

Telegram

@DogepadFinanceCommunity

- 3 189 members
- Active members
- Active mods

Medium

- Not available

SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- ✔ **OVER 150 SUCCESSFUL CLIENTS**

- ✔ **MORE THAN 500 SCAMS EXPOSED**

- ✔ **MILLIONS SAVED IN POTENTIAL FRAUD**

- ✔ **PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS**

- ✔ **CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH**

To hire us, reach out to contact@spywolf.co or t.me/joe_SpyWolf

FIND US ONLINE

🌐 **SPYWOLF.CO**

🌐 **SPYWOLF.NETWORK**

✈ **@SPYWOLFNETWORK**

✈ **@SPYWOLFOFFICIAL**

🐦 **@SPYWOLFNETWORK**

@SPYWOLFNETWORK

14

Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.

While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:

By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.

No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.

The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.

No applications were reviewed for security. No product code has been reviewed.